REMARKS

In the August 3, 2007 Office Action, the Examiner noted that claims 1-10 are pending in the application; rejected claims 8 and 9 under 35 U.S.C. § 112, second paragraph; rejected claim 8 under 35 U.S.C. § 101; rejected claims 1, 3 and 5-10 under 35 U.S.C. § 102(b) as being anticipated by Choo (U.S. Patent No. 6,981,140); rejected claim 2 under 35 U.S.C. § 103(a) as being unpatentable over Choo in view of Iitsuka et al. (U.S. Patent No. 6,463,151); and rejected claim 4 under 35 U.S.C. § 103(a) as being unpatentable over Choo in view of Albrecht et al. (U.S. Patent No. 6,510,521). Claims 1-10 are currently pending in this case. The rejections are traversed below.

Improper Finality

The outstanding final Office Action is improper because the substance of the Applicant's clear traversal in the previous Amendment was not substantially addressed. Following a traversal, the next Office Action is required to expressly address the substance of the Applicant's arguments, as well as new independent claims 9 and 10. 37 C.F.R. § 1.113(b) states that "[i]n making such final rejection, the examiner shall repeat or state all grounds of rejection then considered applicable to the claims in the application, clearly stating the reasons in support thereof." MPEP § 707.07(f) provides that, "[w]here the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and **answer the substance** of it." According to 37 C.F.R. § 1.104(b), the Examiner's answer must be **complete as to all matters**.

With respect to claims 9 and 10, although the Examiner has included these claims in the rejection under 35 U.S.C. § 102(b) on page 5, there is no explanation in the outstanding Office Action of how Choo discloses the limitations of claims 9 and 10. These claims are merely broadly referred to at the beginning of what appears to be a cut-and-pasted copy of claim 1. The limitations recited in claims 9 and 10 differ from those of claim 1 and therefore must be addressed by the Examiner.

Further, the final Office Action does not address the Applicant's argument that Choo discloses neither that "an encryption rule is stored for *each secret level*" (see pages 8 and 9, of the previous Amendment), nor monitoring "whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the *process information* received from the information management system" (see page 9, of the previous Amendment), as recited in claim 1. Thus, the outstanding Office Action fails to meet the requirements of 37 C.F.R. §§ 1.104(b) and 1.113(b), and as such, the finality thereof is improper.

Accordingly, the Applicant respectfully requests withdrawal of the finality of the outstanding Office Action and issuance of a new Office Action, or withdrawal of the rejection of pending claims and allowance of pending claims in view of the claim amendments and remarks herein.

Rejection under 35 U.S.C. § 112

Claims 8 and 9 are rejected under 35 U.S.C. § 112, second paragraph.

In order to more fully comply with the requirements of 35 U.S.C. § 112, second paragraph, claim 8 is amended herein to recite a "computer-readable storage storing a program" instead of a "computer program product".

Claim 9 recites "monitoring whether data is encrypted in accordance with a predetermined encryption rule for a security level" (lines 2 and 3). The Office Action states on page 3 that claim 9 is indefinite because "it is unclear how ... claim 9 can recite 'a predetermined encryption rule'." The Applicant respectfully submits that "a predetermined encryption rule" is not indefinite and particularly points out and distinctly claims the subject matter regarded as the invention.

As stated in MPEP § 2173, "[t]he primary purpose of this requirement of definiteness of claim language is to ensure that the scope of the claims is clear so the public is informed of the boundaries of what constitutes infringement of the patent." As such, definiteness of the claim language is not analyzed in a vacuum, but rather in light of:

(A) The content of the particular application disclosure;
(B) The teachings of the prior art; and
(C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made.

(See MPEP § 2173.02). In determining whether a claim complies with 35 U.S.C. § 112, second paragraph, the Examiner must "consider the claim as a whole to determine whether the claim apprises one of ordinary skill in the art of its scope" (see *Id.*).

An encryption rule is discussed, for example, on pages 12 and 13 of the specification. As a non-limiting example, in some embodiments, an encryption rule may be "an encryption system and update frequency" which is "defined as the encryption rule for each of the encryption ranks A, B, ... [referring to Fig. 5]" (see, for example, page 12, lines 16-19, of the application).

The Applicant respectfully submits that in light of the disclosure in the application, a person of ordinary skill would readily understand what is meant by an encryption rule.

As for the term "predetermined", Dictionary.com defines said term as:

1. to settle or decide in advance.

(Dictionary.com Unabridged (v 1.1), http://dictionary.reference.com/browse/predetermined, based on the Random House Unabridged Dictionary, © Random House, Inc. 2006). As a non-limiting example, the application states, for instance, that in some embodiments:

> The administrator of the policy management server 21 (the system management division) inputs the encryption rule of each encryption rank by operating the terminal device 22 and makes the encryption rank table TB4 as shown in Fig. 5.

(See, for example, page 13, lines 11-15, of the application). In other words, the encryption rule may be entered in advance, or predetermined, by an administrator. Thus, the "predetermined encryption rule" as claimed in claim 9 is clear, defines the metes and bounds of the claimed subject matter, and satisfies the requirements of 35 U.S.C. § 112, second paragraph.

In view of the above, it is respectfully submitted that the rejection is overcome.

Rejection under 35 U.S.C. § 101

Claim 8 is rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

Claim 8 is amended herein to recite a computer-readable storage storing a program. In view of the foregoing, it is respectfully submitted that the rejection is overcome.

Rejection under 35 U.S.C. § 102

Claims 1, 3 and 5-10 are rejected under 35 U.S.C. § 102(b) as being anticipated by Choo (U.S. Patent No. 6,981,140).

Claim 1 recites "an encryption rule storing portion that stores rule information that indicates an encryption rule of the information for each secret level that is a level of wanting to keep information secret" (lines 5-7). The previous Amendment traversed the Examiner's arguments with respect to this feature, but in the outstanding Office Action, the Examiner did not address the substance of the Applicant's arguments. Thus, the arguments that Choo fails to disclose this feature are resubmitted for consideration below.

Page 5 of the Office Action states that the security policy database 602 in Fig. 6 of Choo "inherently stores an encryption rule", citing column 11, lines 3-6. The cited portion of Choo discusses "a security policy, comprising a predetermined set of rules for dealing with data packets, is stored in a security policy database 605 and is accessible by the internet protocol security stack 510" (column 11, lines 3-6). However, claim 1 recites that an encryption rule is stored for *each secret level*. Dictionary.com defines "each" as:

1. every one of two or more considered individually or one by one.

(Dictionary.com Unabridged (v 1.1) based on the Random House Unabridged Dictionary, © Random House, Inc. 2006). Thus, claim 1 recites that there is **more than one** secret level. Conversely, Choo describes that user applications and processes "depicted as residing within memory compartment 603 are all processes and/or files and/or data having the **same** level of security" (column 10, lines 54-57, emphasis added). Choo only describes one level of security and as such, does not disclose the above features of claim 1.

Claim 1 also recites "a monitoring portion that monitors whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the process information received from the information management system" (lines 14-16). The previous Amendment traversed the Examiner's arguments with respect to this feature, but in the outstanding Office Action, the Examiner did not address the substance of the Applicant's arguments. Thus, the arguments that Choo fails to disclose this feature are resubmitted for consideration below.

Page 6 of the Office Action contends that column 10, line 65 through column 11, line 3, column 13, lines 14-20 and Fig. 10 disclose the above feature, stating that "the internet protocol security stack 510 in Fig. 6 is inherently the monitoring portion for monitoring whether the encrypted data received is processed according to the rule/policy prior to transmission."

However, when establishing inherency, the Examiner must provide rationale or evidence tending to show inherency. *See* MPEP 2112 (IV). In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art. *Ex parte Levy,* 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original). Per the above, the Office Action has not provided such a fact or technical reasoning.

Further, before a reference can be found to disclose a feature by virtue of its inherency, one of ordinary skill in the art viewing the reference must understand that the unmentioned feature at issue is necessarily present in the reference. *Continental Can*, 948 F.2d at 1268-69, 20 USPQ 2d at 1749-50. In this case, one of ordinary skill in the art viewing the reference would not understand that the unmentioned feature at issue is necessarily present in the reference. Rather, one of ordinary skill in the art would understand that Choo discusses sending data packets to be transmitted to an internet protocol security stack. (See column 10, lines 65-66) In addition, "every data packet to be transmitted must, in order to conform with the internet protocol security protocol, be checked by the internet protocol security stack 510 against a security policy database associated with key database 602" (column 10, line 66 through column 11, line 3, of Choo). "If it is determined that the received data packet is to be encrypted, then in step 1030, the data packet is encrypted and, in step 1040, returned to the protocol stack via port 509" (column 13, lines 17-20, of Choo).

Therefore, one of ordinary skill in the art would clearly understand that Choo does not monitor whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the *process information* received from the information management system (see, for example, Fig. 15 and page 20, line 2 through page 21, line 25, of the application). On the other hand, per the above, one of ordinary skill in the art would clearly understand that each packet in Choo is simply checked against a security policy database.

Thus, based upon the above-mentioned discussion, the Office Action does *not* meet its burden of proof to establish that the internet protocol security stand 510 in Fig. 6 is inherently the monitoring portion for monitoring whether the encrypted data received is processed according to the rule/policy to transmission.

Claim 1 further recites "a warning portion that warns the information management system that was found to encrypt information not in accordance with the rule by the monitoring portion to do encryption of information in accordance with the rule" (lines 17-19). It is respectfully submitted that Choo fails to disclose this feature.

Page 3 of the Office Action states that:

> Choo teaches that a warning portion for warning the information management system that was found to encrypt information not in accordance with the rule by monitoring portion to do encryption of information in accordance with the rule [column 11, lines 3-25 and fig. 6, the internet protocol security stack 510 warns/detects that it has not received a security association for transferring a particular type of data].

The cited section of Choo discusses that:

> If internet protocol security stack 510 detects that it has not received a security association for transferring a particular type of data, for example, to a remote host then internet protocol security stack 510 instructs an Internet Key Exchange (IKE) block 604 to initiate a negotiation procedure with a corresponding respective internet keying agent associated with the remote host across a LAN/WAN 605.

(Column 11, lines 7-13). In other words, when no security association is received, a remote internet keying agent is contacted and negotiation ensues to obtain the security association. Obtaining a "security association" when one is not found is not the same as "warning", as recited in claim 1. Thus, Choo fails to anticipate claim 1 under 35 U.S.C. § 102(b).

Claim 3 depends from claim 1 and adds further limitations thereto. Thus, the arguments above with respect to claim 1 also apply to claim 3.

Claim 5 recites a classification secret level storing portion that stores classification of information managed by the information management system for each classification in connection with the secret level and a process information transmitting portion that transmits process information that indicates the encryption process performed by the encrypting portion to the encryption support system so as to receive a check whether or not the encryption of the information was performed in accordance with the rule. Thus, claim 5 also patentably distinguishes over Choo.

Claim 6 recites an encryption rule storing portion that stores rule information that indicates an encryption rule of the information for each secret level that is a level of wanting to keep information secret, a monitoring portion that monitors whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the process information received from the information management system, and a warning portion that warns the information management system that was found to encrypt information not in accordance with the rule by the monitoring portion to do encryption of information in accordance with the rule. Thus, claim 6 also patentably distinguishes over Choo.

Claim 7 depends from claim 6 and adds further limitations thereto.

Claim 8 recites transmitting rule information that indicates an encryption rule of the information for each secret level that is a level of wanting to keep information secret and encryption data that is necessary for encrypting information in accordance with the rule to the information management system, monitoring whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the process information received from the information management system, and warning the information management system that was found to encrypt information not in accordance with the rule by the monitoring means to do encryption of information in accordance with the rule. Thus, claim 8 also patentably distinguishes over Choo.

Claim 9 recites monitoring whether data is encrypted in accordance with a predetermined encryption rule for a security level and producing a warning if the data is not encrypted in accordance with the encryption rule. This claim is lumped into the rejection of claim 1, but there is no discussion of which parts of Choo the Examiner relies on in rejecting claim 9. The Applicant again submits that claim 9 distinguishes over Choo and respectfully requests that the Examiner specifically explain which portions of Choo he believes to disclose the claimed features if the rejection is maintained.

Claim 10 recites monitoring whether an information management system encrypts data in accordance with an encryption rule associated with a security level of the information management system and warning the information management system if the data is not encrypted in accordance with the encryption rule. This claim is also lumped into the rejection of claim 1, but again there is no discussion of which parts of Choo the Examiner relies on in rejecting claim 10. The Applicant again submits that claim 10 distinguishes over Choo and respectfully requests that the Examiner specifically explain which portions of Choo he believes to disclose the claimed features if the rejection is maintained.

In view of the above, it is respectfully submitted that the rejection is overcome.

Rejections under 35 U.S.C. § 103

Claim 2 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Choo in view of Iitsuka et al. (U.S. Patent No. 6,463,151).

Claim 2 depends from claim 1 and adds further limitations thereto. It is respectfully submitted that Iitsuka et al. does not teach or suggest modification of Choo to overcome the deficiencies of Choo discussed above. Thus, the arguments above pertaining to claim 1 also apply to claim 2.

In view of the above, it is respectfully submitted that the rejection is overcome.

Claim 4 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Choo in view of Albrecht et al. (U.S. Patent No. 6,510,521).

Claim 4 depends from claim 1 and adds further limitations thereto. It is respectfully submitted that Albrecht et al. does not teach or suggest modification of Choo to overcome the deficiencies of Choo discussed above. Thus, the arguments above pertaining to claim 1 also apply to claim 4.

In view of the above, it is respectfully submitted that the rejection is overcome.

New Claim

Claim 11 is new. Claim 11 emphasizes an encryption rule storing portion that stores rule information that indicates an encryption rule for encrypting information for each encryption rank corresponding to the importance of the information under an encryption policy, which is not taught or suggested by the references, taken alone or in combination thereof. Claim 11 further emphasizes a monitoring portion that monitors whether or not the encryption of information is performed in accordance with the encryption rule by the information management system on the basis of the process information received from the information management system, and a compliance portion that orders the information management system, if found not to encrypt information in accordance with the encryption rule, to encrypt information in accordance with the encryption rule, which is not taught or suggested by the references, taken alone or in combination thereof. Therefore, it is respectfully submitted that claim 11 is patentable over the cited references.

Summary

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 3, 2008

By:
Sheetal S. Patel
Registration No. 59,326

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501